MONOTONICITY OF THE QUANTUM LINEAR PROGRAMMING BOUND

Eric M. Rains

AT&T Research

February 17, 1998

Abstract. The most powerful technique known at present for bounding the size of quantum codes of prescribed minimum distance is the quantum linear programming bound. Unlike the classical linear programming bound, it is not immediately obvious that if the quantum linear programming constraints are satisfiable for dimension K, that the constraints can be satisfied for all lower dimensions. We show that the quantum linear programming bound *is* monotonic in this sense, and give an explicitly monotonic reformulation.

Introduction

The most powerful technique known at present for bounding the size of quantum codes of prescribed minimum distance is the quantum linear programming bound:

Theorem (Quantum LP bound). *If there exists a quantum code encoding K states in n qubits, with minimum distance d, then there exist homogeneous polynomials $A(x,y)$, $B(x,y)$, and $S(x,y)$ of degree n, satisfying the equations*

$$B(x,y) = A(\frac{x+3y}{2}, \frac{x-y}{2}) \tag{1}$$

$$S(x,y) = A(\frac{x+3y}{2}, \frac{y-x}{2}) \tag{2}$$

$$A(1,0) = K^2 \tag{3}$$

$$B(1,y) - \frac{1}{K}A(1,y) = O(y^d) \tag{4}$$

and the inequalities

$$A(x,y) \geq 0 \tag{5}$$

$$B(x,y) - \frac{1}{K}A(x,y) \geq 0 \tag{6}$$

$$S(x,y) \geq 0, \tag{7}$$

where $P(x,y) \geq 0$ means that the polynomial P has nonnegative coefficients.

Proof. This is theorem 10 of [3]; see also [5]. The polynomials $A(x,y)$, $B(x,y)$, and $S(x,y)$ are the weight enumerator, dual weight enumerator, and shadow enumerator, respectively, of the quantum code. □

Key words and phrases. quantum codes linear programming.

Remark. In the sequel, we will use the standard notation $((n,K,d))$ to denote a quantum code encoding K states in n qubits, with minimum distance d.

It is clear that the existence of an $((n,K,d))$ code implies the existence of an $((n,K',d))$ code for all $K' \leq K$, which suggests that the same should be true for the quantum LP bound, namely that if the quantum LP constraints can be satisfied for $((n,K,d))$, then they can be satisfied for $((n,K',d))$ for all $K' \leq K$. At first glance, this appears to be false; after all, in the inequality (6), decreasing K actually makes the inequality *harder* to satisfy. This impression is misleading, however; as we will see below, the quantum LP bound is indeed monotonic in K.

1. Random subcodes

The reason the quantum LP bound "ought" to be monotonic in K is that if $\mathcal{Q}$ is an $((n,K,d))$ code, and $\hat{\mathcal{Q}}$ is a subcode of $\mathcal{Q}$ of dimension K', then $\hat{\mathcal{Q}}$ is an $((n,K',d))$ code. Of course, in general, it is impossible to deduce the weight enumerator of $\hat{\mathcal{Q}}$ from the weight enumerator of $\mathcal{Q}$, so this is not directly applicable to the LP bound. However, if instead of picking a specific subcode, we instead average over *all* subcodes of a given dimension, the resulting average weight enumerator turns out to depend only on the original weight enumerators.

Recall that if $\mathcal{Q}$ is an $((n,K,d))$ code, and $P_{\mathcal{Q}}$ is the orthogonal projection onto $\mathcal{Q}$, then the weight enumerators $A_{\mathcal{Q}}(x,y)$ and $B_{\mathcal{Q}}(x,y)$ are defined by

$$A_{\mathcal{Q}}(x,y) = \sum_{e \in \mathcal{E}} \operatorname{Tr}(P_{\mathcal{Q}} e)^2 x^{n-\operatorname{wt}(e)} y^{\operatorname{wt}(e)},$$
$$B_{\mathcal{Q}}(x,y) = \sum_{e \in \mathcal{E}} \operatorname{Tr}(P_{\mathcal{Q}} e P_{\mathcal{Q}} e) x^{n-\operatorname{wt}(e)} y^{\operatorname{wt}(e)},$$

where $\mathcal{E}$ is the set of all tensor products of matrices from the set $\{I, \sigma_x, \sigma_y, \sigma_x\}$, and $\operatorname{wt}(E)$ is the number of nonidentity tensor factors in E.

Define

$$\hat{A}_{\mathcal{Q}}(x,y) = E_{\hat{\mathcal{Q}} \subset \mathcal{Q}} A_{\hat{\mathcal{Q}}}(x,y),$$

and similarly for $\hat{B}_{\mathcal{Q}}(x,y)$, where the expectation is over subcodes of dimension K'. If we write $P_{\mathcal{Q}} = \Pi\Pi^\dagger$ for some $2^n \times K$ matrix Π, then

$$P_{\hat{\mathcal{Q}}} = \Pi P' \Pi^\dagger,$$

for some $K \times K$ projection operator P' with $\operatorname{Tr}(P') = K'$. So

$$\hat{A}_{\mathcal{Q}}(x,y) = E_{P'} \sum_{e \in \mathcal{E}} |\operatorname{Tr}(\Pi P' \Pi^\dagger e)|^2 x^{n-\operatorname{wt}(e)} y^{\operatorname{wt}(e)},$$

and similarly for $\hat{B}_{\mathcal{Q}}$. But

$$\begin{aligned} E_{P'} \operatorname{Tr}(\Pi P' \Pi^\dagger e)^2 &= E_{U \in U(K)} \operatorname{Tr}(\Pi U P' U^\dagger \Pi^\dagger e)^2 \\ &= E_{U \in U(K)} \operatorname{Tr}(\Pi^\dagger e \Pi U P' U^\dagger)^2. \end{aligned}$$

At this point, we can apply the following lemma:

Lemma 1. *Define functions*

$$s_2(A) = \frac{1}{2}(\mathrm{Tr}(A)^2 + \mathrm{Tr}(A^2))$$
$$s_{1^2}(A) = \frac{1}{2}(\mathrm{Tr}(A)^2 - \mathrm{Tr}(A^2)).$$

For any $K \times K$ matrices A and B,

$$E_{U\in U(K)} s(AUBU^\dagger) = \frac{s(A)s(B)}{s(I_K)},$$

where s is either s_2 or s_{1^2}.

Proof. This follows from the theory of zonal polynomials [1]. For A and B unitary, the relations follow from the fact that s_2 and s_{1^2} are irreducible characters of the unitary group. Since they are also polynomial functions of A and B, the relations must hold for arbitrary matrices. □

In particular,

$$\begin{aligned} E_{U\in U(K)} \mathrm{Tr}(\Pi^\dagger e \Pi U P' U^\dagger)^2 &= E_{U\in U(K)} s_2(\Pi^\dagger e \Pi U P' U^\dagger) + s_{1^2}(\Pi^\dagger e \Pi U P' U^\dagger) \\ &= \frac{K'^2 + K'}{K^2 + K} s_2(\Pi^\dagger e \Pi) + \frac{K'^2 - K'}{K^2 - K} s_{1^2}(\Pi^\dagger e \Pi). \end{aligned}$$

It follows that

$$\hat{A}_{\mathcal{Q}}(x,y) = \frac{K'(K'K-1)}{K^3-K} A_{\mathcal{Q}}(x,y) + \frac{K'(K-K')}{K^3-K} B_{\mathcal{Q}}(x,y).$$

Similarly,

$$\hat{B}_{\mathcal{Q}}(x,y) = \frac{K'(K-K')}{K^3-K} A_{\mathcal{Q}}(x,y) + \frac{K'(K'K-1)}{K^3-K} B_{\mathcal{Q}}(x,y).$$

In general, if $A(x,y)$ is a polynomial satisfying the quantum LP constraints for $((n,K,d))$, then for any $K' \leq K$, we can define

$$\hat{A}(x,y) = \frac{K'(K'K-1)}{K^3-K} A(x,y) + \frac{K'(K-K')}{K^3-K} B(x,y).$$

The claim is that $\hat{A}$ satisfies the quantum LP constraints for K'. We have:

$$\begin{aligned} \hat{A} &= \frac{K'^2}{K^2} A + \frac{K'(K-K')}{K^3-K}(B - \frac{1}{K}A) \\ \hat{B} - \frac{1}{K'}\hat{A} &= \frac{K'^2 - 1}{K^2 - 1}(B - \frac{1}{K}A) \\ \hat{S} &= \frac{K'^2 + K'}{K^2 + K}\left(\frac{S(x,y) + S(-x,y)}{2}\right) + \frac{K'^2 - K'}{K^2 - K}\left(\frac{S(x,y) - S(-x,y)}{2}\right) \end{aligned}$$

Since all of the constants appearing above are positive for $K' \leq K$, and $\hat{A}(1,0) = K'^2$, the claim follows. So we have proved:

Theorem 1. *The quantum linear programming bound is monotonic in K for fixed n and d.*

Remark. Similarly, the quantum LP bound for *pure* codes ($A(1,y) = 1 + O(y^d)$) is monotonic in K, since the random subcode operator preserves purity.

We also obtain the following result of independent interest:

Theorem 2. *The average weight enumerator of a random $((n,K))$ quantum code is*

$$A(x,y) = \frac{K(4^nK - 2^n)}{4^n - 1}x^n + \frac{K(K-2^n)}{4^n-1}(x+3y)^n.$$

Proof. We have $A(x,y) = \hat{A}_{\mathcal{H}}$, where $\mathcal{H}$ is the trivial quantum code consisting of the entire Hilbert space, with weight enumerator 4^nx^n. □

A reformulation

Lemma 1 suggests that we should be able to obtain a simpler formulation of the quantum LP bound by considering the polynomials

$$C(x,y) = \frac{A(x,y) + B(x,y)}{K^2 + K},$$
$$D(x,y) = \frac{A(x,y) - B(x,y)}{K^2 - K}$$

(where $D(x,y)$ is only well-defined for $K > 1$). In particular, we have the following result:

Lemma 2. *The polynomials C and D are preserved by the average subcode operator; that is, $\hat{C} = C$ and $\hat{D} = D$.*

So, if we reformulate the quantum LP bound in terms of C and D, the result should be explicitly monotonic, in that a feasible solution for K will itself be a feasible solution for all smaller K.

Theorem 3. *If there exists an $((n,K,d))$ quantum code ($K > 1$), then there exist homogeneous polynomials $C(x,y)$ and $D(x,y)$, satisfying the equations*

$$C(x,y) = C(\frac{x+3y}{2}, \frac{x-y}{2}) \tag{8}$$
$$D(x,y) = -D(\frac{x+3y}{2}, \frac{x-y}{2}) \tag{9}$$
$$C(1,0) = 1 \tag{10}$$
$$C(1,y) - D(1,y) = O(y^d) \tag{11}$$

and satisfying the inequalities

$$C(x,y) - \frac{K-1}{2K}(C(x,y) - D(x,y)) \geq 0 \tag{12}$$
$$C(x,y) - D(x,y) \geq 0 \tag{13}$$
$$C(\frac{x+3y}{2}, \frac{y-x}{2}) \geq 0 \tag{14}$$
$$D(\frac{x+3y}{2}, \frac{y-x}{2}) \geq 0. \tag{15}$$

Proof. We have

$$A(x,y) = K^2 C(x,y) - \frac{K^2-K}{2}(C(x,y) - D(x,y))$$
$$B(x,y) - \frac{1}{K}A(x,y) = \frac{K^2-1}{2}(C(x,y) - D(x,y))$$
$$S(x,y) = \frac{K^2+K}{2}C(\frac{x+3y}{2}, \frac{y-x}{2}) + \frac{K^2-K}{2}D(\frac{x+3y}{2}, \frac{y-x}{2}).$$

Equations (8) and (9) are clearly equivalent to (1), while (10) and (11) are together equivalent to (3) and (4). Similarly, the inequalities (12) and (13) are equivalent to (5) and (6) respectively.

For (14) and (15), it suffices to note that (8) and (9) imply

$$C(\frac{x+3y}{2}, \frac{y-x}{2}) = C(\frac{-x+3y}{2}, \frac{y+x}{2})$$
$$D(\frac{x+3y}{2}, \frac{y-x}{2}) = -D(\frac{-x+3y}{2}, \frac{y+x}{2})$$

It follows that the two terms in the expression for $S(x,y)$ have disjoint support. So (7) becomes (14) and (15). □

Theorem 1 is an obvious corollary; K appears only in (12), and decreasing K in that equation only makes the constraint easier to satisfy. For pure codes, the additional constraint $C(1,y) = 1 + O(y^d)$ holds, and again monotonicity is obvious.

It should also be noted that this theorem carries over readily to nonbinary codes (from the inequalities in [2]and [4]); in particular, the quantum LP bound is monotonic for larger alphabet codes as well.

References

1. A. T. James, *Zonal polynomials of the real positive definite symmetric matrices*, Ann. of Math. **74** (1961), 475–501.
2. E. M. Rains, *Polynomial invariants of quantum codes*, LANL e-print quant-ph/9704042.
3. E. M. Rains, *Quantum shadow enumerators*, LANL e-print quant-ph/9611001.
4. E. M. Rains, *Quantum weight enumerators*, IEEE Trans. Inf. Th. (to appear).
5. P. W. Shor and R. Laflamme, *Quantum analog of the MacWilliams identities in classical coding theory*, Phys. Rev. Lett. **78** (1997), 1600–1602.

AT&T Research, Room C290, 180 Park Ave. Florham Park, NJ 07932-0971, USA
E-mail address: rains@research.att.com